REMARKS

The Office Action mailed July 11, 2005 has been carefully considered. Reconsideration in view of the following remarks is respectfully requested.

Claim Status and Amendment to the Claims

Claims 1-45 are now pending in the present Application. Of these claims, Claims 1, 10, 12, 21, 23, 32, 34, 35, and 44 have been canceled, without prejudice or disclaimer of the subject matter contained therein.

Examiner's Response to the Applicant's Arguments Filed May 5, 2005 Regarding the 35 U.S.C. §§ 102 and 103 Rejections

In response to the Applicant's arguments filed May 5, 2005 regarding the 35 U.S.C. §§ 102 and 103 rejections, the Examiner states:

> First of all, in HTTP, the Web browser establishes a connection to a Web server and sends an HTTP request message to the server. In response to an HTTP request message, performs any requested action, and returns an HTTP response message containing an HTML document in accord with the requested action, or an error message. The returned HTML document may simply be a file stored on the Web server, or may be created dynamically using a script called in response to the HTTP request message. For instance, to retrieve a document, a Web browser may send an HTTP request message to the indicated Web server, requesting a document by reference to the URL of the document. The Web server then retrieves the document and returns it in an HTTP response message to the Web browser. Request messages in HTTP contain a "method name" indicating the type of action to be performed by the server, a URL indicating a target object (either document or script) on the Web server, and other control information. The request methods defined in the current version of the HTTP protocol include GET, POST, PUT, HEAD, DELETE, LINK, and UNLINK. HEAD, DELETE, LINK and UNLINK are less commonly used. The GET method causes the server to retrieve the object indicated by the given URL and send it back to the client. If the URL refers to a document, then the server responds by sending back the document. If the URL refers to an executable script, then the server executes the script and returns the data produced by the execution of the script. Web browser programs normally use the GET method to send request messages to

> the Web server to retrieve HTML documents, which the Web browser then displays on the screen at the client computer. The POST method sends data, usually the user input parameters from an HTML form, to the server. The POST request also contains the URL of a script to be run on the server. The server runs the script, passing the parameters given in the request, and the script generates an HTML output that is returned in the response to the client. In order for a client program to send arbitrary data to the Web server using the current HTTP protocol, the client program must use either the PUT method or the POST method, as these are the only two methods that allow such data transfer to the Web server. Web browsers generally use only the POST method and generally only for the purpose of sending data in connection with forms to be processed. That is why it is called session establishment requests as taught by the reference Lin.[1]

The Examiner does not provide a specific reference to support the above statements, and support for the statements cannot be found in Lin et al. To the extent the Examiner applies the above statements to the 35 U.S.C. § 102 rejections, the Applicants respectfully submit such a rejection is improper, as each and every element as set forth in the claims are not found, either expressly or inherently described, in a *single* prior art reference. Furthermore, to the extent the Examiner applies the same statements to the 35 U.S.C. § 103 rejections, the Applicants assume that the Examiner intended to take official notice of facts under M.P.E.P. 2144.03 that the rationale supporting the obviousness rejection is based on common knowledge in the art or "well-known" prior art. Under M.P.E.P. 2144.03, "[i]f the applicant traverses such an assertion the examiner should cite a reference in support of his or her position." The Applicants hereby traverse the assertion and request that a reference be cited in support of the position outlined in the Office Action.

[1] Office Action dated July 11, 2005, ¶ 3.

The 35 U.S.C. § 102 Rejection

Claims 2, 5, 13, 16, 24, and 27 stand rejected under 35 U.S.C. § 102(e) as being allegedly anticipated by Lin et al.[2] This rejection is respectfully traversed.

According to the M.P.E.P., a claim is anticipated under 35 U.S.C. § 102(a), (b) and (e) only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.[3] Additionally, "The identical invention must be shown in as complete detail as is contained in the ... claim."[4]

Claim 2

Claim 2 recites:

A method for preventing denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, the method comprising:
receiving a HTTP request from a subscriber having an established connection over a first communication network coupled to at least one other communication network, said request including a Universal Resource Locator (URL);
receiving a profile for said subscriber;
filtering said request to determine whether said subscriber is authorized to make said request based upon said profile, said filtering including:
updating a client HTTP request count when said request for said URL is a HTTP GET request or a HTTP POST request; and
applying HTTP server denial of service attack preventative measures when a client HTTP request frequency based on said client HTTP request count exceeds a maximum HTTP request frequency; and
forwarding said request to said at least one other communication network when said subscriber is authorized to make said request.

The Examiner states:

[2] U.S. Patent No. 6,751,668.
[3] Manual of Patent Examining Procedure (MPEP) § 2131. See also *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).
[4] *Richardson v. Suzuki Motor Co.*, 869 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). *See also*, M.P.E.P. §2131.

> . . . The reference teaches a method for preventing denial of service attacks (col.1, lines 7-10) against Hypertext Transfer Protocol (HTTP) servers (col. 2, lines 17-25) the method comprising:
> receiving a HTTP request from a subscriber using a first communication network coupled to at least one other communication network. said request including a Universal Resource Locator (URL), (col.2, lines 21-25)
> receiving a profile for said subscriber; filtering said request to determine whether said subscriber is authorized to make said request based upon said profile, (col.2, lines 63-66, col.4, lines 14-18) said filtering including:
> updating a client HTTP request count when said request is a HTTP "GET" request or a HTTP "POST" request; and applying HTTP server denial of service attack preventative measures when a client HTTP request frequency based on said client HTTP request count exceeds a maximum HTTP request frequency and forwarding said request to said at least one other communication network when said subscriber is authorized to make said request. (col.2, lines 26-62, col.4, lines 14-18).[5]

The Applicants respectfully disagree. Contrary to the Examiner's statement, Lin et al. does not teach receiving a HTTP request *from a subscriber having an established connection* over a first communication network coupled to at least one other communication network, said request including a Universal Resource Locator (URL). It is noted that the Examiner's statement fails to include the "having an established connection" limitation recited in Claim 2. Additionally, nowhere does Lin et al. refer to a "subscriber", let alone a subscriber having an established connection as recited in Claim 2.

Also contrary to the Examiner's statement, Lin et al. does not teach receiving a profile for said subscriber. In fact, nowhere does Lin et al. refer to a "profile", let alone a profile for a subscriber as recited in Claim 2. The Examiner is reminded that the mere absence from a reference of an explicit requirement of a claim cannot be reasonably construed as an affirmative statement that the requirement is in the reference.[6]

---

[5] Office Action, ¶ 5.
[6] *In re Evanega*, 829 F.2d 1110, 4 USPQ2d 1249 (Fed. Cir. 1987).

The Examiner is further reminded that a proper rejection under 35 U.S.C. § 102 requires that the identical invention must be shown in as complete detail as is contained in the claim. Such a showing has not been made in the present case.

Also contrary to the Examiner's statement, Lin et al. does not teach filtering said request to determine whether said subscriber is authorized to make said request based upon said profile. As discussed above, Lin et al. teaches neither a subscriber having an established connection, nor a profile for the subscriber. Consequently, Lin et al. cannot be said to teach filtering said request to determine whether said subscriber is authorized to make said request based upon said profile.

Also contrary to the Examiner's statement, Lin et al. does not teach updating a client HTTP request count when said request for said URL is a HTTP GET request or a HTTP POST request. Nowhere does Lin et al. refer to a HTTP GET request or a HTTP POST request. Rather, Lin et al. teaches a session request may be a TCP SYN packet, or a new UDP or ICMP packet.[7]

Also contrary to the Examiner's statement, Lin et al. does not teach forwarding said request to said at least one other communication network when said subscriber is authorized to make said request. As mentioned above, Lin et al. does not teach filtering said request to determine whether said subscriber is authorized to make said request based upon said profile. Nor does Lin et al. teach receiving a HTTP request from a subscriber having an established connection over a first communication network coupled to at least one other communication

[7] Lin et al. col. 2 ll. 5-6.

network. Thus, Lin et al. cannot be said to teach forwarding said request to said at least one other communication network when said subscriber is authorized to make said request.

The Examiner also states:

> Lin is effervescent in elucidating that "receiving a HTTP request from a subscriber having an established connection over a first communication network coupled to at least one other communication network. said request including a Universal Resource Locator (URL)", in col. 2, line 10-25, "A filter 106 operates to selectively block session establishment packets 108 from being provided to the target 104. In particular, an abnormally high number of session establishment attempts is usually an indication that a denial of service (DoS) attack is occurring. The filter 106 records the total number of existing sessions and measures the rate of session requests of each stream. A "stream" is a data traffic flow between a particular source and a specific target. A source could be a single host, a group of hosts in a network or domain, or any number of hosts in the entire Internet. By the same token, a target could involve one or more hosts and servers in an internal network. However, the most likely scenario of a DoS attack occurs from an arbitrary host in the Internet to a specific site in an internal network. This specific site is usually represented by a single domain name or a virtual IP (VIP) address."
>
> Lin thereby teaches that Dos includes the existing sessions to a specific site in an internal network represented by a single domain name or virtual IP (VIP) address.[8]

The Applicants respectfully disagree. Contrary to the Examiner's statement, Lin et al. can hardly be said to be "effervescent" in elucidating limitations in claims of the present Application, particularly when Lin et al. is devoid of such limitations. Again, Lin et al. mentions neither HTTP requests, nor receiving such requests from subscribers having an established connection over a first communication network coupled to at least one other communication network.

The Examiner also states:

> Lin also teaches in col. 2, line 63-66, "By selectively passing some of the session establishment requests, the filter 106 allows at least some legitimate session requests to get through to the target 104 (unlike the prior art "total blocking" method)."
>
> Lin thereby teaches that Dos includes the existing sessions to a specific site in an internal network represented by a single domain name or virtual IP (VIP) address wherein

[8] Office Action, ¶ 3.

legitimate session request is determined. (The "profile" is used to differentiate one subscriber from another.)[9]

The Applicants respectfully disagree. The passage cited by the Examiner speaks generally about allowing a number of legitimate session *requests* to get through to a target. The passage provides no support for the Examiner's conclusion regarding *existing* sessions. Furthermore, the Examiner's parenthetical reference to a "profile" finds no support in Lin et al.

For the above reasons, the 35 U.S.C. § 102 rejection of claim 2 based on Lin et al. is unsupported by the art and should be withdrawn.

Claim 5

Claim 5 recites:

> The method of claim 2, wherein said applying further comprises dropping the data packet containing said request when said client HTTP request frequency exceeds said maximum HTTP request frequency.

The Examiner states:

> . . . The reference teaches the method wherein said applying further comprises dropping the data packet containing said request when said client HTTP request frequency exceeds said maximum HTTP request frequency. (col. 2, lines 33-39, lines 63-66).[10]

The Applicants respectfully disagree. Again, Li et al. speaks generally about limiting session *establishment* packets, but says nothing of HTTP requests. Thus, the identical invention is not shown in Li et al. in as complete detail as is contained in the claim.

[9] Office Action, ¶ 3.
[10] Office Action, ¶ 5.

For the above reasons, the 35 U.S.C. § 102 rejection of claim 5 based on Lin et al. is unsupported by the art and should be withdrawn.

Independent Claims 13 and 24

Claim 13 is an In re Beauregard claim corresponding to method claim 2. Claim 24 is a means-plus-function claim corresponding to method claim 2. Claim 2 being allowable, Claims 13 and 24 must be allowable for at least the same reasons.

Dependent Claims 16 and 27

Claim 16 depends from Claim 13 and is an In re Beauregard claim corresponding to method claim 5. Claim 27 depends from Claim 24 and is a means-plus-function claim corresponding to method claim 5. Claims 13 and 24 being allowable, Claims 16 and 27 must be allowable for at least the same reasons.

The First 35 U.S.C. § 103 Rejection

Claims 3, 4, 6, 14, 15, 17-20, 25, 26, and 29-31 stand rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Lin et al. in view of Primeaux et al.[11] This rejection is respectfully traversed.

According to the Manual of Patent Examining Procedure (M.P.E.P.),

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or

[11] U.S. Patent No. 6,334,121.

> suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in the applicant's disclosure.[12]

Claims 3, 4, and 6 depend from claim 1 and thus include the limitations of claim 1. Claims 14, 15, and 17-20 depend from claim 13 and thus include the limitations of claim 13. Claims 25, 25, and 29-31 depend from claim 24 and thus include the limitations of claim 24. The arguments made above with respect to claim 1, 13, and 24 apply here as well. The 35 U.S.C. § 102 rejection of claims 1, 13, and 24 based on Li et al. is unsupported by the art, as each and every element as set forth in claims 1, 13, and 24 is not found in Li et al. Therefore, the 35 U.S.C. § 103 rejection of dependent claims 3, 4, 6, 14, 15, 17-20, 25, 26, and 29-31 based on Li et al. in view of Primeaux et al. is also unsupported by the art. Thus, no prima facie case of obviousness has been established and the 35 U.S.C. § 103 rejection should be withdrawn.

Claims 3 and 4

Claim 3 recites:

> The method of claim 2, wherein said applying further comprises setting an alarm when said client HTTP request frequency exceeds said maximum HTTP request frequency.

The Examiner states:

> . . . Keeping in mind the teachings of the reference Lin as stated above, the reference fails to teach setting an alarm when said client HTTP request frequency exceeds said maximum HTTP request frequency and sending said alarm to an Internet Service Provider (ISP) associated with subscriber. The reference Primeaux teaches the action taken could be defined to suspend the user account or merely mail a message to the system administrator (sending alarm to an Internet Service Provider (ISP) associated with subscriber), warning of a potential intruder including the category of users such as Yes--definitely the appropriate user, No--definitely an intruder and Yes/No--may or may not be the appropriate user. (col. 10, lines 50-59). The reference also teaches that if the usage pattern is outside of the user's normal usage pattern, this triggers the system to react

[12] M.P.E.P § 2143.

> automatically. The reaction of the system is adjustable and will depend primarily on the nature and the degree of destructiveness of a particular command and the level of security awareness that the software is set for (dropping the data packet containing request). Various levels of security are determined by the list of commands deemed critical by the system administrator. (col. 10, lines 60-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to combine Lin's capabilities with Primeaux's usage pattern tracking capabilities and applying the attack preventive measures based on the set threshold levels such as client HTTP request frequency exceeding a maximum HTTP request frequency and setting an alarm to the ISP (the system administrator).[13]

The Applicants respectfully disagree. As mentioned above, to establish a prima facie case of obviousness there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. The Examiner has not indicated a suggestion or motivation to combine the reference teachings. For this additional reason, no prima facie case of obviousness has been established and the 35 U.S.C. § 103 rejection of Claim 3 should be withdrawn.

Claim 4

Claim 4 recites:

> The method of claim 3, further comprising sending said alarm to an Internet Service Provider (ISP) associated with said subscriber.

Claim 4 depends from claim 3. Claim 3 being allowable, claim 4 must be allowable for at least the same reasons. Additionally, the Applicants respectfully submit the Examiner's attempt to equate a system administrator as disclosed in Primeaux et al., with an Internet Service Provider, is improper. Thus the prior art references when combined do not teach or suggest all

[13] Office Action, ¶ 6.

the claim limitations. For this additional reason, no prima facie case of obviousness has been established and the 35 U.S.C. § 103 rejection of Claim 4 should be withdrawn.

Claims 6, 7, 8, and 9

Claim 6 recites:

The method of claim 2, wherein said applying further comprises shutting down the account used to access said first communication network when said client HTTP request frequency exceeds said maximum HTTP request frequency.

The Examiner states:

. . . Keeping in mind the teachings of Lin as stated above, although the reference teaches disabling HTTP requests for a hold-down period when said client HTTP request frequency exceeds said maximum HTTP request frequency. (Fig. 4, "shaded area"), the reference fails to teach shutting down the account used to access first communication network when said client HTTP request frequency exceeds said maximum HTTP request frequency and increasing said hold-down period each time said client HTTP request frequency exceeds said maximum HTTP request frequency, and wherein said hold-down period increases exponentially each time said client HTTP request frequency exceeds said maximum HTTP request frequency. The reference Primeaux teaches the action taken could be defined to suspend the user account (shutting down the account used to access and disabling HTTP requests for a hold-down period) or merely mail a message to the system administrator, warning of a potential intruder including the category of users such as Yes--definitely the appropriate user, No--definitely an intruder and Yes/No--may or may not be the appropriate user. (col. 10, lines 50-59). The reference also teaches that if the usage pattern is outside of the user's normal usage pattern, this triggers the system to react automatically. The reaction of the system is adjustable and will depend primarily on the nature and the degree of destructiveness of a particular command and the level of security awareness that the software is set for (hold-down period each time client HTTP request frequency exceeds said maximum HTTP request frequency and hold-down period increases exponentially each time client HTTP request frequency exceeds maximum HTTP request frequency). Various levels of security are determined by the list of commands deemed critical by the system administrator. (col. 10, lines 60-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to combine Lin with Primeaux's usage pattern tracking capabilities based on the normal commands such as a HTTP "GET" request or a HTTP "POST" request; and applying the attack preventive measures based on the set threshold levels such as client HTTP request frequency exceeding maximum HTTP request frequency set by the security rules and to suspend the user account (shutting down the account used to access and disabling HTTP requests for a hold-down period) as desired, based on the level of

> security awareness that the software is set for (hold-down period each time client HTTP request frequency exceeds said maximum HTTP request frequency and hold-down period increases exponentially each time HTTP frequency exceeds maximum HTTP request frequency) when client HTTP request frequency exceeds a maximum HTTP frequency. This provides a system wherein the system will detect a difference in the pattern of usage. When such a difference is detected, the system will take the appropriate action.[14]

Contrary to the Examiner's statement, the combined references teach or suggest an HTTP request frequency, let alone shutting down an account based on an HTTP request frequency. The Examiner uses the following passage in Primeaux et al. in support of the Examiner's rejection of claims 6-9:

> The reaction of the system is adjustable and will depend primarily on the nature and the degree of destructiveness of a particular command and the level of security awareness that the software is set for.[15]

The Applicants respectfully submit the above passage is insufficient to teach or suggest the claimed limitation. Thus the prior art references when combined do not teach or suggest all the claim limitations. For this additional reason, no prima facie case of obviousness has been established and the 35 U.S.C. § 103 rejection of Claim 6 should be withdrawn.

Claim 7 recites:

> The method of claim 6, wherein said applying further comprises disabling HTTP requests for a hold-down period when said client HTTP request frequency exceeds said maximum HTTP request frequency.

Claim 7 depends from claim 6. Claim 6 being allowable, claim 7 must be allowable for at least the same reasons. Additionally, the combined references say nothing about disabling HTTP requests for a hold-down period when a client HTTP request frequency exceeds said

[14] Office Action, ¶ 6.
[15] Primeaux et al. col. 10 ll. 61-65.

maximum HTTP request frequency. Thus the prior art references when combined do not teach or suggest all the claim limitations. For this additional reason, no prima facie case of obviousness has been established and the 35 U.S.C. § 103 rejection of Claim 7 should be withdrawn.

Claim 8 recites:

> The method of claim 7, further comprising increasing said hold-down period each time said client HTTP request frequency exceeds said maximum HTTP request frequency.

The Applicants respectfully disagree. Claim 8 depends from claim 7. Claim 7 being allowable, claim 8 must be allowable for at least the same reasons. Additionally, the combined references say nothing about increasing a hold-down period each time a client HTTP request frequency exceeds a maximum HTTP request frequency. Thus the prior art references when combined do not teach or suggest all the claim limitations. For this additional reason, no prima facie case of obviousness has been established and the 35 U.S.C. § 103 rejection of Claim 8 should be withdrawn.

Claim 9 recites:

> The method of claim 8, wherein said hold-down period increases exponentially each time said client HTTP request frequency exceeds said maximum HTTP request frequency.

The Applicants respectfully disagree. Claim 9 depends from claim 8. Claim 8 being allowable, claim 9 must be allowable for at least the same reasons. Additionally, the combined references say nothing about a hold-down period increasing exponentially each time a client HTTP request frequency exceeds a maximum HTTP request frequency. Thus the prior art references when combined do not teach or suggest all the claim limitations. For this additional

reason, no prima facie case of obviousness has been established and the 35 U.S.C. § 103 rejection of Claim 9 should be withdrawn.

Claims 14-15 and 17-20

Claims 14-15 and 17-20 are In re Beauregard claims corresponding to method claims 3-4 and 6-9, respectively. Claims 3-4 and 6-9 being allowable, Claims 14-15 and 17-20 must be allowable for at least the same reasons.

Claims 25-26 and 28-31

Claims 25-26 and 28-31 are means-plus-function claims corresponding to method claims 3-4 and 6-9, respectively. Claims 3-4 and 6-9 being allowable, Claims 25-26 and 38-31 must be allowable for at least the same reasons.

The Second 35 U.S.C. § 103 Rejection

Claims 36-43 stand rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Lin et al. in view of Primeaux et al.,[16] and further in view of Prabandham et al.[17] This rejection is respectfully traversed.

Claims 36-43 are apparatus claims corresponding to method claims 2-9, respectively. Thus, the arguments made above with respect to Claims 2-9 apply here as well. Claims 2-9 being allowable, claims 36-43 must be allowable for at least the same reasons.

[16] U.S. Patent No. 6,334,121.
[17] U.S. Patent No. 6,701,438.

Regarding Claim 36, the Examiner states:

> . . . The reference Lin teaches a first receiving interface capable of accepting a HTTP request received from a subscriber using a first communication network., said request including a Universal Resource Locator (URL); (Fig. 1, element 106); a profile request generator capable of generating a profile request based upon said request; (col. 2, lines 63-66); a filter capable of determining whether said request is authorized based upon said requested profile. said filter including; an updater to update a client HTTP request count when said request for said URL is a HTTP "GET" request or a HTTP "POST" request, and a responder to apply HTTP server denial of service attack preventative measures when a client HTTP request frequency based on said client HTTP request count exceeds a maximum HTTP request frequency; (col. 2, lines 26-66, col. 4, lines 14-18). Keeping in mind the teachings of the references Lin and Primeaux, both of these references fails to a first forwarding interface capable of sending said profile request to an Authentication, Authorization, and Accounting (AAA) server; a second receiving interface capable of accepting a requested profile; an authorizer capable of allowing said request to be forwarding on at least one other communication network coupled to said first communication network: and a second forwarding interface capable of forwarding said request on said at least one other communication network. The reference Prabandham teaches an authorizer capable of allowing said request said request to be forwarded on at least one other communication network coupled to said first communication network. (Fig. 2, element 216 and col. 4, line 67 and col. 5, lines 1-8); a first forwarding interface capable of sending said profile request to an AAA server; (element 212 which has the first receiving interface which is AAA server); a second receiving inter-face capable of accepting a requested profile; and a second forwarding interface capable of forwarding said request on said at least one other communication network. (element 216's interfaces connected to element 212 and element 206). Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to combine Lin with Primeaux's usage pattern tracking capabilities and Prabandham's security protocols. In this way, it will provide an alternative to the Lin's system for an user AAA verification, in addition to filter's capability to selectively passing some of the session establishment requests.[18]

Again, to establish a prima facie case of obviousness there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. The Examiner has not indicated a suggestion or motivation to combine the reference teachings. For this additional reason, no prima facie case of obviousness has been established and the 35 U.S.C. § 103 rejection of Claim 36 should be withdrawn.

[18] Office Action, ¶ 8.

In view of the foregoing, it is respectfully asserted that the claims are now in condition for allowance.

Conclusion

It is believed that this Amendment places the above-identified patent application into condition for allowance. Early favorable consideration of this Amendment is earnestly solicited.

If, in the opinion of the Examiner, an interview would expedite the prosecution of this application, the Examiner is invited to call the undersigned attorney at the number indicated below.

The Applicants respectfully request that a timely Notice of Allowance be issued in this case. Please charge any additional required fee or credit any overpayment not otherwise paid or credited to our deposit account No. 50-1698.

Respectfully submitted,

THELEN REID & PRIEST, LLP

Dated: August 19 2005

John P. Schaub
Reg. No. 42,125

Thelen Reid & Priest LLP
P.O. Box 640640
San Jose, CA 95164-0640
Tel. (408) 292-5800
Fax. (408) 287-8040